

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年 1 1 月 1 9 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 3 - 3 8 9 2 3 0  
Application Number:  
[ST. 10/C]:                      [ J P 2 0 0 3 - 3 8 9 2 3 0 ]

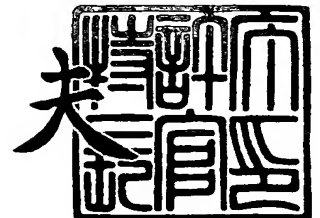
出 願 人                      株式会社日立製作所  
Applicant(s):

U.S. Appln. Filed 2-26-04  
Inventor: Y. Ishii et al  
mattingly stanger & malor  
Docket MEI-101

2 0 0 4 年   2 月   3 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号   出証特 2 0 0 4 - 3 0 0 5 3 1 3



【書類名】 特許願  
【整理番号】 PA20G215  
【提出日】 平成15年11月19日  
【あて先】 特許庁長官 今井 康夫 殿  
【国際特許分類】 G06F 12/00  
【発明者】  
    【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所  
                                システム開発研究所内  
    【氏名】 石井 陽介  
【発明者】  
    【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所  
                                システム開発研究所内  
    【氏名】 藺田 浩二  
【発明者】  
    【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所  
                                システム開発研究所内  
    【氏名】 岩寄 正明  
【特許出願人】  
    【識別番号】 000005108  
    【氏名又は名称】 株式会社日立製作所  
【代理人】  
    【識別番号】 110000028  
    【氏名又は名称】 特許業務法人 明成国際特許事務所  
    【代表者】 下出 隆史  
    【電話番号】 052-218-5061  
【手数料の表示】  
    【予納台帳番号】 133917  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 0111082

**【書類名】 特許請求の範囲****【請求項 1】**

ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、

前記ネットワークには、前記ストレージ装置および前記アクセス制御装置が複数接続されており、

該アクセス制御装置は、

各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、

前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限するアクセス制限部と、

アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける情報入力部と、

前記入力に基づき、前記ネットワークに接続された各アクセス制御装置がそれぞれ参照する前記アクセス禁止リストを更新する処理を行うリスト更新部とを備えるアクセス制御装置。

**【請求項 2】**

請求項 1 記載のアクセス制御装置であって、

前記リスト更新部は、前記他のアクセス制御装置に対して、前記ユーザ情報を該他のアクセス制御装置が参照する前記アクセス禁止リストに登録させる登録指示を配信するアクセス制御装置。

**【請求項 3】**

請求項 1 記載のアクセス制御装置であって、

前記リスト更新部は、前記更新された前記アクセス禁止リストを、前記他のアクセス制御装置へ配信するアクセス制御装置。

**【請求項 4】**

ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、

前記ネットワークには、前記ストレージ装置および前記アクセス制御装置が複数接続されており、

各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、

前記ネットワークに接続された他のアクセス制御装置から、前記各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する受信部と、

前記所定の情報により、前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストを更新するリスト更新部と、

前記アクセスコントロールリストより前記アクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えるアクセス制御装置。

**【請求項 5】**

請求項 1～請求項 4 いずれか記載のアクセス制御装置であって、

前記アクセス制限部は、未完了の処理を含めて、前記アクセス制限を行うアクセス制御装置。

**【請求項 6】**

請求項 1～請求項 5 いずれか記載のアクセス制御装置であって、

前記アクセス禁止リストに基づき、前記アクセスコントロールリストを更新するアクセスコントロールリスト更新部を備えるアクセス制御装置。

**【請求項 7】**

請求項 6 記載のアクセス制御装置であって、

前記アクセス禁止リスト内のユーザ情報を、所定のタイミングで削除するアクセス制御装置。

**【請求項 8】**

請求項 7 記載のアクセス制御装置であって、  
前記所定のタイミングとは、前記アクセスコントロールリスト更新部における前記更新の終了後であるアクセス制御装置。

【請求項 9】

請求項 7 記載のアクセス制御装置であって、  
前記所定のタイミングとは、前記ネットワークに接続された全てのアクセス制御装置における、前記アクセスコントロールリスト更新部における前記更新の終了後であるアクセス制御装置。

【請求項 10】

情報資源を格納するストレージ装置と、情報資源のアクセスを制御するためのアクセス制御装置とが、ネットワークに複数接続されたアクセス制御システムであって、

各アクセス制御装置は、

各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、

前記アクセスコントロールリストより、前記情報資源へのアクセスを禁止すべきユーザを特定可能な所定の情報を登録したアクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えており、

いずれか一のアクセス制御装置は、自装置が参照する前記アクセス禁止リストに変更が発生した場合に、前記所定の情報、または、前記アクセス禁止リストを、前記ネットワークに接続された他のアクセス制御装置に配信する配信部を備え、

前記他のアクセス制御装置は、前記所定の情報、または、前記アクセス禁止リストを受信し、自装置が参照するアクセス禁止リストを更新するリスト更新部を備えるアクセス制御システム。

【請求項 11】

請求項 10 記載のアクセス制御システムであって、

前記配信部は、前記他のアクセス制御装置へ、前記アクセス禁止リストを更新するための更新情報を同報配信するアクセス制御システム。

【請求項 12】

請求項 10 記載のアクセス制御システムであって、

前記アクセス禁止リストを更新するための更新情報を最初に配信するアクセス制御装置の前記配信部は、前記アクセス禁止リストを更新するための更新情報を、予め設定された他のアクセス制御装置へ配信し、

前記他のアクセス装置の配信部は、受信した前記更新情報を、更に、予め設定された他のアクセス制御装置へ配信するアクセス制御システム。

【請求項 13】

ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御方法であって、

前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されており、

各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う工程と、

前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限する工程と、

アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける工程と、

前記入力に基づき、前記ネットワークに接続された各アクセス制御装置がそれぞれ参照する前記アクセス禁止リストを更新する処理を行う工程とを備えるアクセス制御方法。

【請求項 14】

ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御方法であって、

前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されて

おり、

各情報資源のアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う工程と、

前記ネットワークに接続された他のアクセス制御装置から、前記各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する工程と、

前記所定の情報により、前記アクセス禁止リストを更新する工程と、

前記アクセスコントロールリストより前記アクセス禁止リストを優先してアクセスを制限する工程とを備えるアクセス制御方法。

【請求項 15】

情報資源を格納するストレージ装置と、該オブジェクトへのアクセスを制御するためのアクセス制御装置とが、ネットワークに複数接続されたアクセス制御システムにおいてアクセスを制御するアクセス制御方法であって、

各アクセス制御装置は、

各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行うアクセス判断部と、

前記アクセスコントロールリストより、前記情報資源へのアクセスを禁止すべきユーザを特定可能な所定の情報を登録したアクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えており、

いずれかのアクセス制御装置は、自装置が参照する前記アクセス禁止リストに変更が発生した場合に、前記所定の情報、または、前記アクセス禁止リストを、前記ネットワークに接続された他のアクセス制御装置に配信する工程を備え、

前記他のアクセス制御装置は、前記所定の情報、または、前記アクセス禁止リストを受信し、自装置が参照するアクセス禁止リストを更新する工程を備えるアクセス制御方法。

【請求項 16】

ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスをコンピュータに制御させるためのコンピュータプログラムであって、

前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されており、

各情報資源へのアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う機能と、

前記情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限する機能と、

アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける機能と、

前記入力に基づき、前記ネットワークに接続された各アクセス制御装置がそれぞれ参照する前記アクセス禁止リストを更新する処理を行う機能とをコンピュータに実現させるためのコンピュータプログラム。

【請求項 17】

ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスをコンピュータに制御させるためのコンピュータプログラムであって、

前記ネットワークには、前記ストレージ装置およびアクセス制御装置が複数接続されており、

各情報資源のアクセス可否が登録されたアクセスコントロールリストに基づき、アクセス可否の判断を行う機能と、

前記ネットワークに接続された他のアクセス制御装置から、前記各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する機能と、

前記所定の情報により、前記アクセス禁止リストを更新する機能と、

前記アクセスコントロールリストより前記アクセス禁止リストを優先してアクセスを制限する機能とをコンピュータに実現させるためのコンピュータプログラム。

【請求項 18】

請求項 16 または請求項 17 記載のコンピュータプログラムをコンピュータ読み取り可

能に記録した記録媒体。

**【書類名】 明細書****【発明の名称】** ブラックリストによる緊急アクセス遮断装置**【技術分野】****【0001】**

本発明は、コンピュータに保存された情報資源へのアクセス制御に関するものである。

**【背景技術】****【0002】**

従来、コンピュータに蓄積された情報資源を利用するに際し、情報資源と利用者とを対応付けて設定されたアクセス権限を登録したアクセスコントロールリストによりアクセス制限を行うことにより、セキュリティの向上を図っている。近年では、インターネットなどの広域ネットワークを介して、複数のネットワークを接続し、ファイルなどの資源を共有する分散環境を構築した超分散環境が普及しつつある。かかる環境においても、アクセスコントロールリストが使用されている。アクセスコントロールリストは、各ネットワークに存在するアクセス制御装置に管理されており、全てのネットワークのアクセス制御装置間で同期が取られている。

**【0003】**

情報資源へのアクセス権限は、固定的なものではなく、種々の状況に応じて変化する。例えば、超分散環境において、特定のユーザの全アクセスを遮断しなければならない状況が発生した場合には、全てのアクセスコントロールリストに対して、アクセス権限を停止する旨の更新を同期的に行うことにより、特定のユーザのアクセスを遮断する、という技術が開示されている（特許文献1）。また、アクセス権限を認証する認証局により発行される証明書を、定期的に通知することにより、失効した証明書を持つユーザのアクセスを遮断する、という技術も開示されている（非特許文献1）。

**【0004】**

**【特許文献1】** 特開平11-282805号公報

**【非特許文献1】** アイ・イー・ティー・エフ アール・エフ・シー3280：“インターネットX.509パブリックキー インフラストラクチャー サーティフィケート アンド サーティフィケート リボケーション リスト (シー・アール・エフ) プロファイル” (IETF RFC 3280：“Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”) 2002年4月

**【発明の開示】****【発明が解決しようとする課題】****【0005】**

しかしながら、例えば、解雇によるアクセス権限削除や、第3者による不正アクセスが発覚した場合など、緊急にアクセス遮断を実現しなければならない状況が発生した場合に、特許文献1記載の技術では、アクセスコントロールリストの更新に、非常に時間がかかり、緊急アクセス遮断を実現することは困難である場合がある。また、非特許文献1記載の技術においても、証明書の発行間隔、すなわち、証明書の更新間隔が定期的であり、発行間隔によっては、緊急アクセス遮断を実現することは困難であるという問題があった。

**【0006】**

これらの課題は、超分散環境に特化した課題ではなく、複数のアクセス制御装置が連携してアクセス制御を行う場合の共通の課題であった。

**【課題を解決するための手段】****【0007】**

上述の課題の少なくとも一部を解決するために、本発明は第1の構成として、以下の態様をとることとした。すなわち、ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、ネットワークには、ストレージ装置およびアクセス制御装置が複数接続されており、かかるアクセス制御装置は、各情報資源へのアクセス可否が登録されたアクセスコントロールリスト（以下「ACL

」と呼ぶこととする)に基づき、アクセス可否の判断を行うアクセス判断部と、全ての情報資源へのアクセスを禁止するユーザを特定可能な情報が登録されたアクセス禁止リストに基づき、アクセスを制限するアクセス制限部と、アクセス禁止ユーザを特定可能なユーザ情報の入力を受け付ける情報入力部と、入力に基づき、ネットワークに接続された各アクセス制御装置がそれぞれ参照するアクセス禁止リストを更新する処理を行うリスト更新部とを備えることを要旨とする。

#### 【0008】

アクセス禁止ユーザを特定可能な情報とは、例えば、ユーザID、ユーザ名等が挙げられる。また、例えばIPアドレスなど、ユーザが利用している端末を特定する情報としてもよい。ACLには、例えば、読み取り専用、削除禁止、など詳細なアクセス権限の設定がされていることとしてもよいし、単に、アクセス許可、不許可が設定されていることとしても良い。

#### 【0009】

情報入力部は、例えば、ユーザから、キーボードなどの入力装置による直接入力を受け付けることとしてもよいし、アクセス禁止ユーザの登録されたファイルを読み込むことにより入力することとしてもよい。また、アクセス禁止リストそのものを取得することとしてもよい。リスト更新部は、例えば、アクセス禁止リストに登録されているユーザ情報を書き換えることにより更新することとしてもよいし、アクセス禁止リスト自体を差し替えることにより更新することとしてもよい。

#### 【0010】

このような構成をとることにより、複数のネットワークが、インターネットなどの広域ネットワークを介して接続されている超分散環境において、緊急アクセス遮断を行う必要のあるユーザ情報を、全てのネットワークのアクセス制御装置に通知することができ、緊急アクセス遮断を実現することができる。また、ACLは、情報資源ごとにアクセス許可が設定されているため、設定情報は膨大であり、更新処理に非常に時間がかかるが、アクセス禁止リストは、情報資源とは無関係にユーザ単位で全アクセスを禁止することとしており、データ量が軽いため、通知、更新処理の負荷を軽減することができる。

#### 【0011】

本発明のアクセス制御装置において、リスト更新部は、他のアクセス制御装置に対して、ユーザ情報を他のアクセス制御装置が参照する前記アクセス禁止リストに登録させる登録指示を配信することとしてもよい。こうすれば、ネットワークの負荷を軽減することができる。好適である。

#### 【0012】

本発明のアクセス制御装置において、リスト更新部は、更新されたアクセス禁止リストを、他のアクセス制御装置へ配信することとしてもよい。こうすれば、受信側のアクセス制御装置は、アクセス禁止リストを差し替えるだけで更新することができ、処理効率を向上することができる。

#### 【0013】

本発明の第2の構成として、ネットワークに複数接続されたストレージ装置に格納される情報資源へのアクセスを制御するアクセス制御装置であって、ネットワークには、ストレージ装置およびアクセス制御装置が複数接続されており、各情報資源のアクセス可否が登録されたACLに基づき、アクセス可否の判断を行うアクセス判断部と、ネットワークに接続された他のアクセス制御装置から、各情報資源へのアクセスを禁止するユーザを特定可能な所定の情報を受信する受信部と、所定の情報により、アクセス禁止リストを更新するリスト更新部と、ACLよりアクセス禁止リストを優先してアクセスを制限するアクセス制限部とを備えることを要旨とする。

#### 【0014】

こうすれば、他のネットワークでアクセス禁止ユーザの登録要求が発生した場合にも、自ネットワークのアクセス制御装置に存在するアクセス禁止リストに、アクセス禁止ユーザを特定可能な所の情報を速やかに反映させることができる。従って、超分散環境におい



て、緊急アクセス遮断を効率的に実現することができる。

【0015】

本発明の第1の構成および第2の構成におけるアクセス制御装置において、アクセス制限部は、未完了の処理を含めて、アクセス制限を行うこととしてもよい。こうすれば、アクセス禁止リスト更新後のアクセスのみでなく、アクセス禁止リスト更新前にアクセスされ開始された処理や、アクセス待ちの処理までも遮断することができ、利便性が向上する。

【0016】

本発明の第1の構成および第2の構成におけるアクセス制御装置において、アクセス禁止リストに基づき、ACLを更新するACL更新部を備えることとしてもよい。こうすれば、改めてACLを更新するための処理を行う必要がなく、利便性の向上を図ることができる。

【0017】

本発明のアクセス制御装置において、前記ACL更新後、前記アクセス禁止リスト内のユーザ情報を、所定のタイミングで削除する削除部を備えることとしてもよい。

【0018】

例えば、アクセス禁止リストに一度登録されたユーザ情報が削除されないこととなると、アクセス禁止リストの内容が膨大となり、アクセス禁止リストの確認に時間を浪費する恐れがある。そのため、本発明のように、ACLの更新後に、アクセス禁止リストに登録されているユーザ情報を削除することとすれば、アクセス禁止リストの肥大を回避することができ、アクセス遮断処理の遅延を回避することが可能となる。また、アクセス禁止リスト自体を削除することとしても、本発明は実現可能である。

【0019】

本発明のアクセス制御装置において、所定のタイミングとは、アクセス制御装置ごとに、ACLの更新の終了後としてもよい。こうすれば、各ネットワークに存在するアクセス制御装置は、個別に、ACLに更新済みのアクセス禁止ユーザ情報を削除することができる。アクセス制御装置は、ACLに先立ち、アクセス禁止リストを参照するため、本発明のように、ACLの更新終了を契機として、アクセス禁止リストに登録されているユーザ情報を削除することとすれば、アクセス制御装置の処理負荷を軽減することができる。

【0020】

本発明のアクセス制限装置において、所定のタイミングとは、ネットワークに接続された全てのアクセス制御装置における、更新の終了後であることとしてもよい。

【0021】

こうすれば、全てのアクセス制御装置で、ACLおよびアクセス禁止リストの同期を確保することができる。この方法は、例えば、アクセス禁止リスト自体が配信され、差し替えることによりアクセス禁止リストを更新する態様の場合に、有用性が高い。一部のアクセス制御装置においてACLの更新が終了していないにも関わらず、新しいアクセス禁止リストが配信されることによる既存のアクセス禁止リストの内容のACLへの反映漏れを回避することができる。本発明によれば、このような問題を回避しつつ、同期のとられたACLによって、アクセス遮断を行うことができる。

【0022】

本発明は、また、第1の構成および第2の構成のアクセス制御装置を組合せ、第1の構成のアクセス制御装置は、自装置が参照する前記アクセス禁止リストに変更が発生した場合に、所定の情報、または、前記アクセス禁止リストを、前記ネットワークに接続された他のアクセス制御装置に配信する配信部を備え、第2の構成のアクセス制御装置は、所定の情報、または、アクセス禁止リストを受信し、自装置が参照するアクセス禁止リストを更新するリスト更新部を備えるアクセス制御システムとして構成することとしてもよい。

【0023】

所定の情報を通知することとすれば、ネットワークに負荷をかけることなく処理を実行でき、処理効率を向上することができる。また、アクセス禁止リストを通知することとす

れば、緊急アクセス遮断を要するユーザが複数発生した場合には一度に通知することができ、また、アクセス禁止リスト自体を差し替えることで更新処理を行うことができるため、受信側のアクセス制御装置の処理負荷を軽減することができる。

#### 【0024】

本発明のアクセス制御システムにおいて、配信部は、他のアクセス制御装置へ、アクセス禁止リストを更新するための更新情報を同報配信することとしてもよい。こうすれば、全てのアクセス制御装置に対してまとめて通知することができ、好適である。

#### 【0025】

本発明のアクセス制御システムにおいて、アクセス禁止リストを更新するための更新情報を最初に配信するアクセス制御装置の配信部は、アクセス禁止リストを更新するための更新情報を、予め設定された他のアクセス制御装置へ配信し、かかる更新情報を受信した他のアクセス制御装置の配信部は、更に、予め設定された他のアクセス制御装置へ配信することとしてもよい。こうすれば、ネットワークのホップ数などを考慮した配信を行うことができ、利便性が向上する。

#### 【0026】

本発明は上述したアクセス制御装置、アクセス制御システムのほかに、アクセス制御方法として構成することもできる。また、上述のアクセス制御装置を実現するコンピュータプログラム、およびそのプログラムを記録した記録媒体、そのプログラムを含み搬送波内に具現化されたデータ信号など種々の態様で実現することが可能である。各態様において、先に示した種々の付加的要素を適用することが可能である。

#### 【0027】

本発明をコンピュータプログラムまたはそのプログラムを記録した記録媒体等として構成する場合には、アクセス制御装置、アクセス制御装置を制御するプログラム全体として構成するものとしてもよいし、本発明の機能を果たす部分のみを構成するものとしてもよい。また、記録媒体としては、フレキシブルディスクやCD-ROM、DVD-ROM、パンチカード、バーコードなどの符号が印刷された印刷物、コンピュータの内部記憶装置（ROMやRAM等のメモリ）および外部記憶装置などコンピュータが読み取り可能な種々の記録媒体を利用できる。

#### 【発明を実施するための最良の形態】

#### 【0028】

以下、本発明の実施の形態について、以下の項目に分けて説明する。

##### A. 実施例：

- A1. システム構成：
- A2. 機能ブロック：
- A3. アクセス制御処理：
- A4. ブラックリスト配信処理：
- A5. アクセス遮断処理：
- A6. ACL更新処理：

##### B. 変形例：

#### 【0029】

##### A. 実施例：

##### A1. システム構成：

図1は、本発明の実施例におけるシステム構成を例示する説明図である。アクセス制御システム1000は、インターネットINTを介して、4つのネットワークA、B、C、Dから構成されている。ネットワークAは、アクセス制御装置100、ストレージ500、クライアントCL1等が、ローカルエリアネットワークLAN1を介して接続されている。ネットワークB、C、Dも同様に、アクセス制御装置200、300、400と、ストレージ600、700、800と、クライアントCL2、CL3、CL4とが、それぞれ、ローカルエリアネットワークLAN2、LAN3、LAN4を介して接続されている。

## 【0030】

各ストレージには、データファイル501, 601, 701, 801等が格納されており、アクセス制御システム1000は、インターネットINTを介した、いわゆる、超分散環境を構築している。各クライアントは、自己が接続されているネットワークのストレージ装置のみでなく、他のネットワークに接続されたストレージ装置内に格納されているデータファイルを参照することができる。すなわち、クライアントCL1は、ストレージ500内のデータファイル501にアクセスすることができるだけでなく、ネットワークCに存在するストレージ700内のデータファイル701にアクセスすることもできる。

## 【0031】

各ストレージ内のデータファイルにアクセスするためには、アクセス権限の許否が判断される。かかるアクセス権限の許否の判断は、アクセス制御装置が行う。クライアントCL1がデータファイル501にアクセス要求を行うと、アクセス制御装置1000は、クライアントCL1のユーザの、データファイル501へのアクセス権限の許否確認を要求し、かかる確認結果に基づき、データファイルへのアクセスを制御する。

## 【0032】

アクセス制御装置1000は、データファイルなどのオブジェクトのアクセス権限がユーザごとに詳細に設定されたアクセスコントロールリスト110（以降、ACL110と呼ぶこととする）と、ACL110に登録されておらず、緊急に全てのアクセスを禁止する必要のあるユーザ情報が登録されたアクセス禁止リスト120（以降、「ブラックリスト120」と呼ぶこととする）とを管理している。アクセス制御装置1000は、アクセス要求を受け付けると、まず、アクセス要求を行ったユーザのユーザ情報がブラックリスト120に登録されているか否かを判断し、登録されていない場合には、ACL110を参照してアクセス許否を判断する。

## 【0033】

アクセス制御装置1000は、ネットワークAで、例えば解雇によるアクセス権限削除など、緊急にアクセスを遮断する必要のあるユーザが発生した場合に、管理者の操作に応じて、自己のブラックリスト120を更新し、他のアクセス制御装置200, 300, 400に対して、かかるユーザ情報を、それぞれのブラックリスト220, 320, 420へ登録させる指示を配信する。アクセス制御装置200, 300, 400は、かかる登録指示を受信して、自己のブラックリスト220, 320, 420を更新する。こうすることによって、超分散環境において、緊急アクセス遮断を必要とするユーザが発生した場合にも、全てのネットワークで、効率的に緊急アクセス遮断を行うことができる。

## 【0034】

A2. 機能ブロック:

図2は、アクセス制御装置1000の機能ブロックを例示する説明図である。アクセス制御装置1000は、主制御部101と、通信部102と、ACL管理部103と、ブラックリスト管理部104と、アクセス制御部105と、アクセス制御部105の一部として構成されているアクセス制限部106と、アクセス遮断部107と、入力部108と、ストレージ管理部109とから構成されている。通信部102は、アクセス制御装置1000が接続されているローカルエリアネットワークLAN1内の他の器機との通信、インターネットINTを介した他のネットワークとの通信等を制御する。

## 【0035】

ACL管理部103は、オブジェクト毎に、ユーザの詳細なアクセス権限を登録したACL110を管理しており、ACL110の更新等を行う。ACL110の詳細は後述する。ブラックリスト管理部104は、解雇など、緊急にアクセスを遮断する必要のあるユーザが発生した場合、かかるユーザのユーザIDとユーザ名が登録されるブラックリスト120を管理する。登録されるユーザIDおよびユーザ名は、管理者により、入力部108を介して入力される。ブラックリスト120の内容は後述する。ACL管理部103は、また、情報の授受を行いながら、ブラックリスト120に登録されているユーザ情報により、ACL110を更新する機能を奏する。アクセス制御装置1000は、本来ACLの

みによりアクセス制御を行うことが処理効率の観点からも好ましいため、ブラックリスト 120 に登録されたアクセス遮断が必要なユーザ情報に基づき、ACL 110 から遮断対象ユーザに関する情報を削除する。

#### 【0036】

ストレージ管理部 109 は、アクセス制御装置 100 と同一ネットワーク、すなわち、ローカルエリアネットワーク LAN 1 に接続されているストレージ 500 等のストレージ装置を管理する。具体的には、各ストレージに格納されているデータ情報や、各ストレージ装置にアクセスしているユーザ等を管理している。図にアクセスの状態を表したアクセス管理表 109a を併せて示した。

#### 【0037】

アクセス管理表 109a は、各アクセスに固有に割り振られたアクセス ID と、オブジェクト名称と、アクセス状態と、アクセスユーザとから構成されている。例えば、ジョブ ID 「1」のオブジェクト「O-9」は、「アクセス中」であり、アクセスしているユーザは「S-3」であることを示している。同様に、アクセス ID 「2」のオブジェクト「O-7」は、「アクセス待ち」であり、ユーザは「S-8」であることを示している。

#### 【0038】

アクセス制御部 105 は、ACL 110 によるアクセス制限や、緊急アクセス遮断などアクセスに関する処理を制御する機能を奏する。アクセス制御部 106 は、アクセス制御部 105 の一部として構成されており、ユーザのアクセス権限の確認要求を受け付けると、ACL 110 を参照して、結果をストレージ 500 に通知する。アクセス遮断部 107 は、同じく、アクセス制御部 105 の一部として構成されており、ブラックリスト 120 、および、アクセス管理表 109a を参照して、アクセス管理表 109a に存在するユーザが、ブラックリスト 120 に登録されているユーザ、すなわち、緊急にアクセスを遮断しなければならないユーザである場合には、アクセス中、アクセス待ちに関わらず、即座に遮断する機能を奏する。例えば、ユーザ ID 「S-1」のユーザが、ブラックリスト 120 に登録されている場合には、アクセス ID 「3」および「6」のアクセスが遮断されることとなる。

#### 【0039】

図 3 (a) は、本実施例における ACL を例示する説明図である。ACL 110 は、設定されたアクセス権限に固有に割り振られた「ID」と、オブジェクト名を示す「オブジェクト」と、管理ユーザ名を示す「ユーザ」と、アクセス可能なグループを表す「グループ」と、アクセス権限を示す「アクセス」とから構成される。グループを図 3 (b) に示した。破線で示されるグループ「G-1」には、ユーザ ID が「S-1」、「S-2」、「S-3」、「S-4」、「S-5」というユーザが含まれる。更に、一点鎖線に示すようにグループ「G-2」は、「G-1」の一部であり、ユーザ「S-1」、「S-2」、「S-5」が含まれる。ユーザ「S-1」、「S-2」、「S-5」は、グループ「G-1」および「G-2」の双方に属することとなる。

#### 【0040】

アクセス権限は、図 3 (a) の右下に示すように、「R」は「Read」すなわち「読み取り可能」を表しており、「W」は「Write」すなわち「書き込み可能」を表している。例えば、ID 「1」のオブジェクト「O-1」は、ユーザ「S-3」により「R、W」すなわち、読み取り、書き込みが可能であることを示している。また、ID 「2」に示すように、オブジェクト「O-1」は、更に、グループ「G-1」に属するユーザに、「R」すなわち「読み取り可能」というアクセスを認めていることとなる。

#### 【0041】

図 4 は、本実施例におけるブラックリスト 120 の内容を例示する説明図である。ブラックリスト 120 は、ユーザ ID と、ユーザ名とから構成される。ユーザ ID、ユーザ名のいずれかのみから構成されることとしてもよい。本実施例では、アクセス制御装置 100 でアクセス遮断要求を受け付け、ユーザ ID 「S-1」、ユーザ名「Tar o Hit a c h i」というユーザのアクセスを遮断すべくブラックリスト 120 に登録した状態を

示した。本実施例では、かかるユーザのみしかブラックリスト120に登録されていないが、一度に複数のユーザを登録することも可能である。また、既にブラックリストに登録されており、新たに、アクセス遮断すべきユーザを追加することも可能である。

#### 【0042】

他のアクセス制御装置200、300、400も同様の構成であるため、説明は省略する。

#### 【0043】

A3. アクセス制御処理:

図5は、本実施例におけるアクセス制御処理を説明するチャート図である。クライアントCL1が、ストレージ500内のデータファイル501にアクセスを要求する場合の処理を表している。

#### 【0044】

クライアントCL1は、アクセス制御装置100にアクセス要求を送出する(ステップSa100)。アクセス制御装置100は、かかる要求を受け付け、アクセス権限の確認要求を行い、ブラックリスト120およびACL110に基づき、アクセス許否を判断する(ステップSa101)。アクセス制御装置100は、かかる結果に基づき、ストレージ500にアクセスを行い(ステップSa102)、アクセス結果を、自己を介して(ステップSa103)、クライアントCL1へ通知する(ステップSa104)。

#### 【0045】

図6は、アクセス制御処理を説明するフローチャートである。アクセス制御装置100が行う処理であり、図5のステップSa101に相当する処理である。

#### 【0046】

アクセス制御装置100は、クライアントCL1からストレージ500へのアクセス権限の確認要求を、ユーザID、アクセス対象オブジェクト名とともに受信する(ステップS10)と、ブラックリスト120を参照し(ステップS11)、かかるユーザがブラックリスト120に登録されているか否かを判断する(ステップS12)。ブラックリスト120に登録されている場合には、アクセス遮断対象ユーザであるため、ストレージ500に対して、アクセス不許可通知を送出する(ステップS16)。

#### 【0047】

かかるユーザがブラックリスト120に登録されていない場合には、ACL110を参照し、アクセス対象オブジェクトのアクセス許否の詳細を確認する(ステップS13)。アクセス制御装置100は、アクセス許否を判断し(ステップS14)、アクセスが許可されている場合(ステップS14: YES)には、読み取り可能、書き込み可能などのアクセス制限内容に基づき、ストレージ500にアクセスする(ステップS15)。ブラックリスト120には登録されていない(ステップS12: NO)が、ACL110において、アクセスが許可されていない場合(ステップS14: NO)には、クライアントCL1に対してアクセス不許可通知を送出する(ステップS16)。

#### 【0048】

A4. ブラックリスト配信処理:

図7は、本実施例におけるブラックリスト配信処理を説明するフローチャートである。アクセス制御装置100は、アクセス遮断要求を管理者から受け付けると、自己のブラックリスト120に、アクセス遮断対象ユーザのユーザ情報を登録するとともに、かかるユーザ情報の登録指示を、アクセス制御装置200、300、400に対して一度に送出する。図7では、説明の便宜上、アクセス制御装置100からアクセス制御装置200に登録指示が送出される処理を示した。

#### 【0049】

アクセス制御装置100は、アクセス遮断要求を管理者から受け付ける(ステップS20)と、アクセス遮断を行うユーザのユーザIDとユーザ名をブラックリスト120へ登録する(ステップS21)。そして、他のネットワークに接続されたアクセス制御装置200、300、400に対して、かかるアクセス遮断対象ユーザを各アクセス制御装置内

のブラックリストへ登録するよう、ユーザIDおよびユーザ名と併せて登録指示を送出する（ステップS22）。

#### 【0050】

次に、アクセス制御装置100は、ブラックリストに登録されたユーザが、ストレージ500内のオブジェクトに、アクセス中、もしくはアクセス待ちの状態である場合、かかるアクセスを即座に遮断する（ステップS23）。そして、ブラックリストに基づき、ACLを更新し（ステップS24）、更新終了後、ブラックリスト120からユーザ情報を削除する（ステップS25）。

#### 【0051】

アクセス制御装置200は、ステップS22において送付された登録指示を受信する（ステップS30）と、ブラックリストにユーザIDとユーザ名を追加し、ブラックリスト220を更新する（ステップS31）。ブラックリスト220の更新を終えると、アクセス遮断すべきユーザのアクセスを遮断し（ステップS32）、ACLを更新して（ステップS33）、ブラックリスト220からユーザ情報を削除する（ステップS34）。ステップS32～ステップS34までの処理は、アクセス制御装置100におけるステップS23～ステップS25と同様である。アクセス遮断処理（ステップS23、ステップS32）およびACL更新処理（ステップS24、ステップS33）については後述する。

#### 【0052】

A5. アクセス遮断処理：

図8は、本実施例におけるアクセス遮断処理を説明するフローチャートである。アクセス制御装置100のアクセス遮断部107が実行する処理であり、図7のステップS23に相当する処理である。図7のステップS32において、アクセス制御装置200が実行する処理も同様である。

#### 【0053】

アクセス制御装置100は、ブラックリスト120およびアクセス管理表109aを参照し（ステップS40、S41）、ブラックリスト120に登録されているユーザが、ストレージ500内のオブジェクトにアクセス中、もしくは、アクセス待ちの状態であるかどうか判断する（ステップS42）。アクセス中、もしくは、アクセス待ちである場合には、かかるユーザのアクセスを、アクセス中、アクセス待ちにかかわらず、すべて遮断する（ステップS43）。アクセス中、もしくは、アクセス待ちオブジェクトが存在しない場合には、処理を終了する。

#### 【0054】

A6. ACL更新：

図9は、本実施例におけるACLを更新する処理を説明するフローチャートである。図7のステップS24に相当する処理である。図7のステップS33において、アクセス制御装置200が実行する処理も同様である。本実施例では、ユーザID「S-1」、ユーザ名「Taro Hitachi」というユーザを、アクセス遮断対象ユーザとした。

#### 【0055】

アクセス制御装置100は、ブラックリスト120およびACL110を参照し（ステップS50）、グループ情報から、ユーザID「S-1」を削除する（ステップS51）。次に、アクセス制御装置100は、ACL110から、ユーザIDが「S-1」であるIDを抽出し削除する（ステップS51）。本実施例では、図に太矢印で示すように、ID「5」が削除される。

#### 【0056】

こうすれば、グループに関する情報を維持しつつ、ユーザID「S-1」が関係するACL110を更新することができる。

#### 【0057】

以上説明した実施例によれば、超分散環境において、あるユーザのアクセス権限を、緊急に停止したい状況が発生した場合に、かかるユーザの情報を全てのネットワークのアクセス制御装置に、速やかに通知することができる。また、図9で説明したように、ACL

を更新するには、多くの工数がかかるため、本発明のようにブラックリストを配置し、ACLより先にブラックリストを参照してアクセス遮断を行うことにより、セキュリティの向上を図ることができる。

#### 【0058】

##### B. 変形例:

以上、本発明の種々の実施例について説明したが、本発明はこれらの実施例に限定されことなくその趣旨を逸脱しない範囲内で種々の構成を取ることができることはいうまでもない。例えば、以下のような変形が可能である。

#### 【0059】

##### B1. 変形例1:

上述した実施例では、アクセス制御装置100から他のアクセス制御装置200, 300, 400へ、アクセス遮断対象ユーザのユーザ情報を、各アクセス制御装置のブラックリストに登録させる登録指示を送出することとしたがこれに限られない。例えば、アクセス制御装置100で更新したブラックリストの複製を他のアクセス制御装置200, 300, 400へ配布することとしてもよい。こうすれば、ブラックリスト受信側のアクセス制御装置は、ブラックリストを差し替えるだけで更新することができ、処理効率を向上することができる。

#### 【0060】

また、上述した実施例では、ACL更新後、ブラックリストに登録されているユーザ情報を削除することとしたが、本変形例のように、ブラックリストを配布する場合には、ブラックリストそのものを削除することとしてもよい。図10に、本変形例におけるブラックリスト削除処理を説明するフローチャートを示した。本変形例では、アクセス制御装置100は、ACLの更新を終了しているものとする。

#### 【0061】

アクセス制御装置200は、ACLの更新を終了する(ステップSa200)と、ブラックリスト配布元のアクセス制御装置100へ、更新終了通知を送出する(ステップSa201)。同様に、アクセス制御装置400およびアクセス制御装置300も、ACLの更新を終了すると、更新終了通知を送出する(ステップSa202～ステップSa205)。

#### 【0062】

アクセス制御装置100は、他のアクセス制御装置の全てから更新終了通知を受信すると、自己のブラックリストを削除する(Sa207)と共に、他のアクセス制御装置にブラックリストの削除指示を送出し、かかる削除指示を受信した他のアクセス制御装置200, 300, 400は、ブラックリストを削除する(ステップSa208～Sa214)。

。

#### 【0063】

このような構成をとることにより、全てのアクセス制御装置において、ACLの同期を取ることができる。例えば、連続して緊急アクセス遮断要求が発生し、短時間に複数回ブラックリストの配布が行われるような場合には、ACLにユーザ情報が未反映の状態のブラックリストが、後続のブラックリストによって更新されることを回避することができる。

。

#### 【0064】

##### B2. 変形例2:

上述の実施例では、アクセス制御装置100から他のアクセス制御装置200, 300, 400へ、同時にブラックリストを配布することとしたが、これに限られない。例えば、図11に示すように、各アクセス制御装置は、ブラックリストを、予め設定された他のアクセス制御装置へ逐次的に配信することとしてもよい。図に太線矢印で示すように、アクセス制御装置100は、ブラックリストをアクセス制御装置200へ配信し、アクセス制御装置200はアクセス制御装置300に配信し、アクセス制御装置300は、アクセス制御装置400へ配信する。こうすれば、ネットワークのホップ数などを考慮した配信

を行うことができ、利便性が向上する。

【0065】

B 3. 変形例 3：

また、例えば、上述した実施例の超分散環境に、更に、ユーザが正規のユーザであることを証明する証明書を管理する認証局を設置することとしてもよい。かかる場合には、認証局において、証明書の認証に先立ち、ブラックリストによるアクセス制御を行うこととすれば、セキュリティを向上することができ、好適である。

【図面の簡単な説明】

【0066】

【図 1】 本実施例におけるシステム構成図である。

【図 2】 本実施例におけるアクセス制御装置の機能ブロック図である。

【図 3】 本実施例におけるアクセスコントロールリストを例示する説明図である。

【図 4】 本実施例におけるブラックリストを例示する説明図である。

【図 5】 本実施例におけるアクセス制御処理を説明するチャート図である。

【図 6】 本実施例におけるアクセス制御処理を説明するフローチャートである。

【図 7】 本実施例におけるアクセス権限確認処理を説明するフローチャートである。

【図 8】 本実施例におけるアクセス遮断処理を説明するフローチャートである。

【図 9】 本実施例における A C L 更新処理を説明するフローチャートである。

【図 10】 変形例におけるブラックリスト削除処理を説明するフローチャートである。

。

【図 11】 変形例におけるシステム構成図である。

【符号の説明】

【0067】

1 0 0 0... アクセス制御システム

1 0 0, 2 0 0, 3 0 0, 4 0 0... アクセス制御装置

1 1 0, 2 1 0, 3 1 0, 4 1 0... A C L

1 2 0, 2 2 0, 3 2 0, 4 2 0... ブラックリスト

5 0 0, 6 0 0, 7 0 0, 8 0 0... ストレージ

5 0 1, 6 0 1, 7 0 1, 8 0 1... データファイル

1 0 1... 主制御部

1 0 2... 通信部

1 0 3... A C L 管理部

1 0 4... ブラックリスト管理部

1 0 5... アクセス制御部

1 0 6... アクセス制限部

1 0 7... アクセス遮断部

1 0 8... 入力部

1 0 9... ストレージ管理部

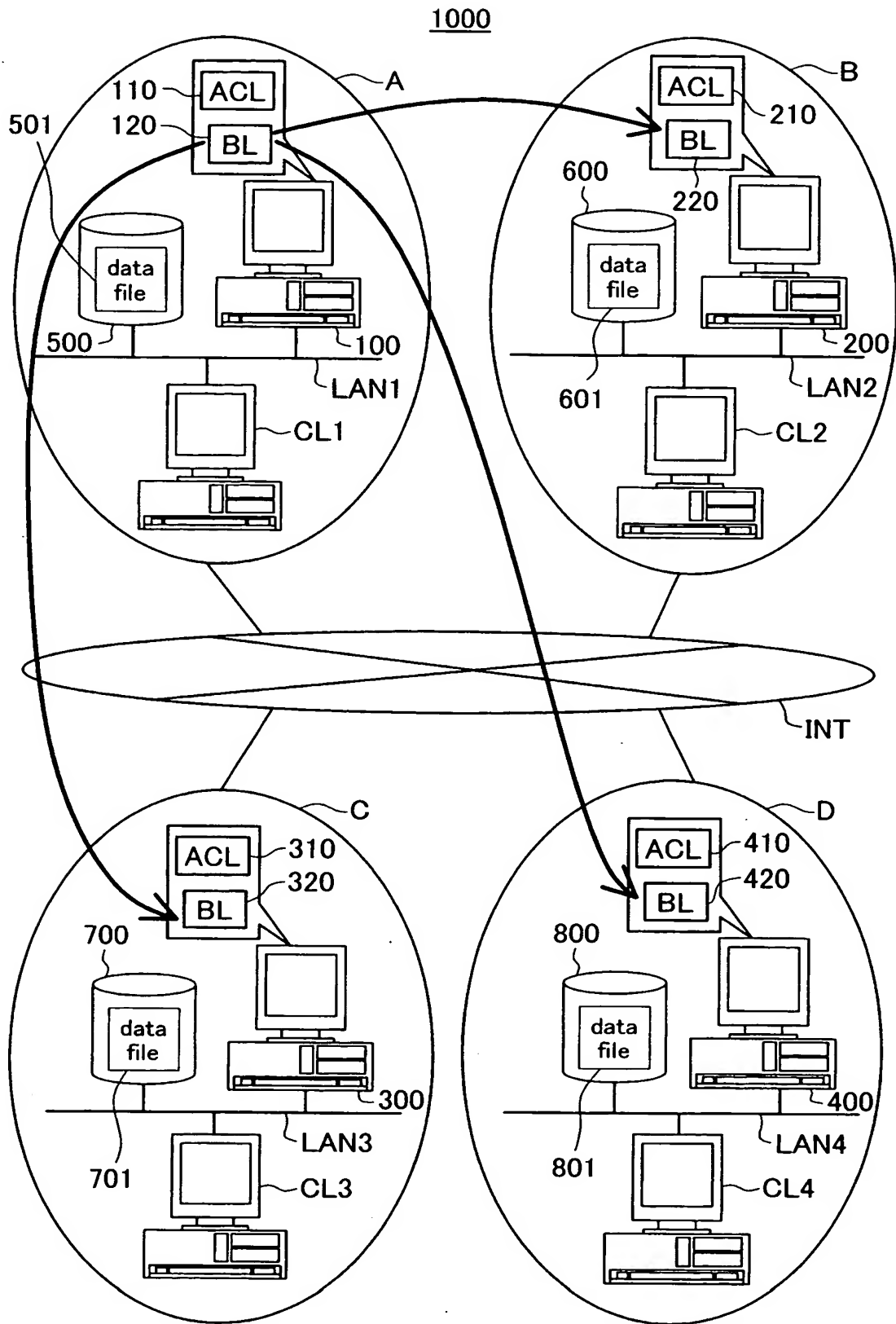
1 0 9 a... アクセス管理表

1 1 0... アクセスコントロールリスト

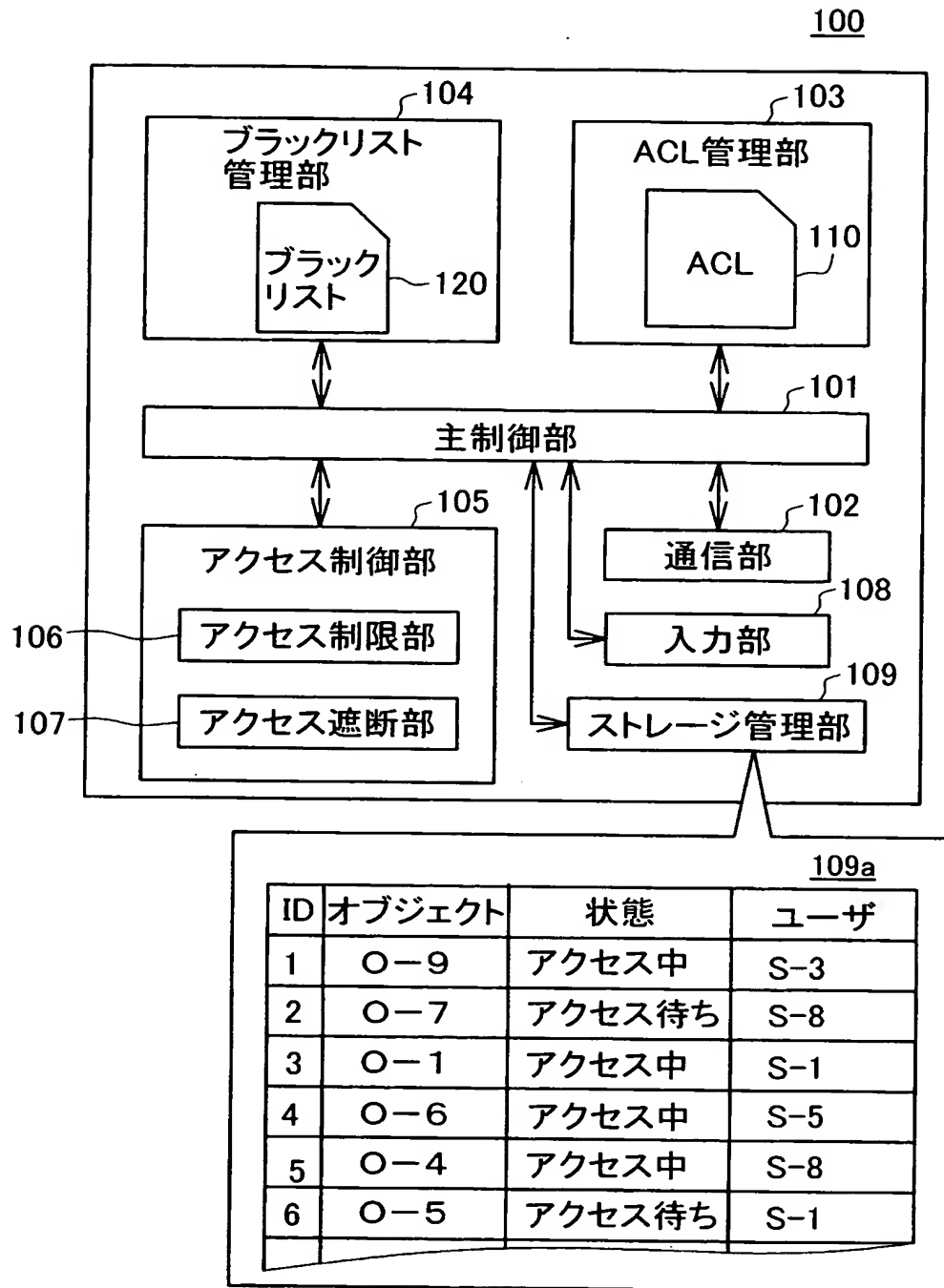
1 2 0... ブラックリスト



【書類名】 図面  
【図 1】



【図 2】



【図 3】

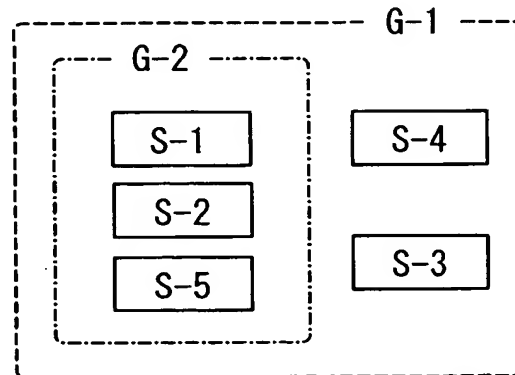
(a)

110

ID	オブジェクト	ユーザ	グループ	アクセス
1	0-1	S-3	—	R, W
2	0-1	—	G-1	R
3	0-2	S-7	—	R, W
4	0-2	—	G-2	R
5	0-3	S-1	—	R, W
6	0-3	—	G-2	R

R-Read  
W-Write

(b)

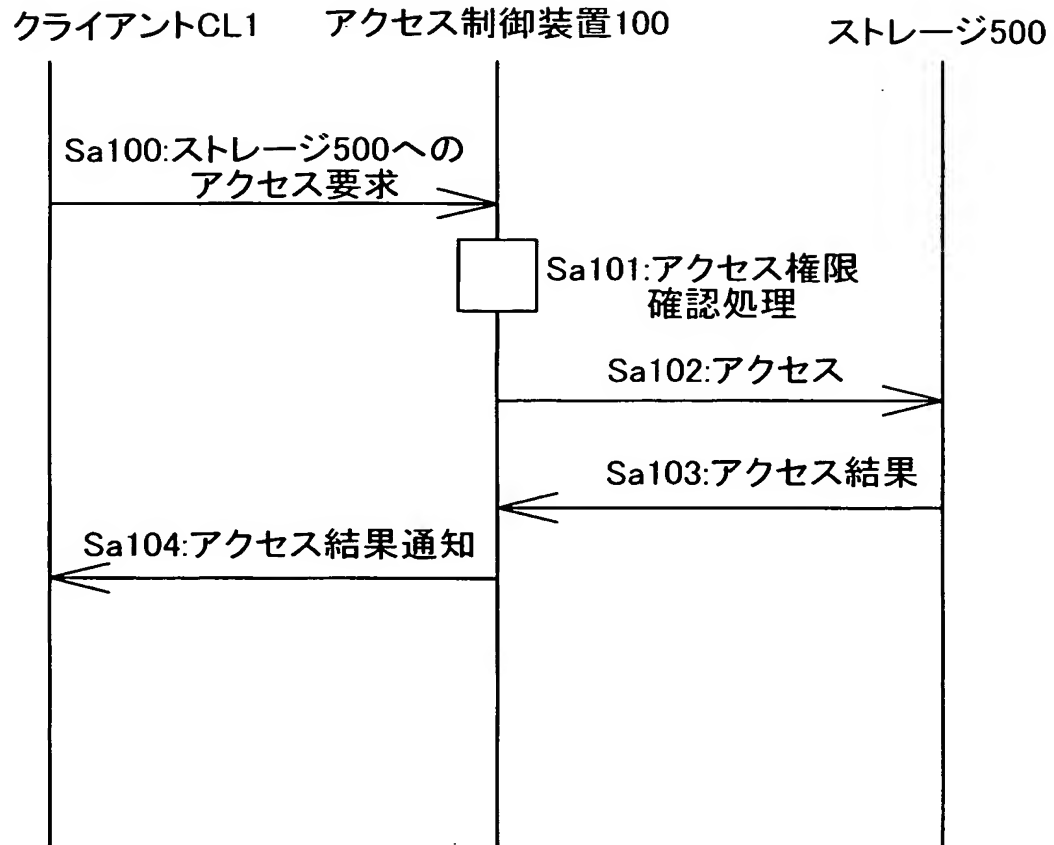


【図 4】

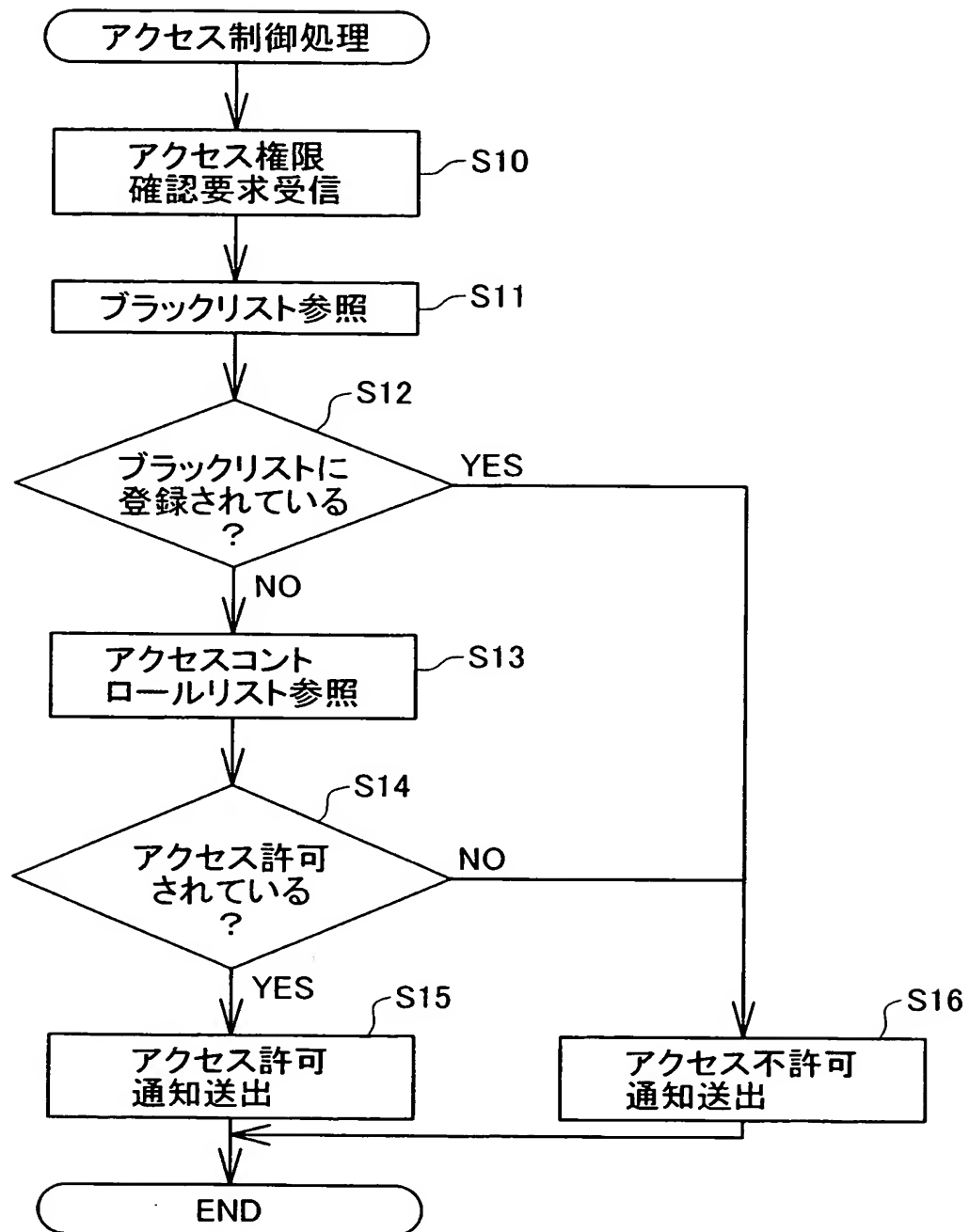
120

User ID	User Name
S-1	Taro Hitachi

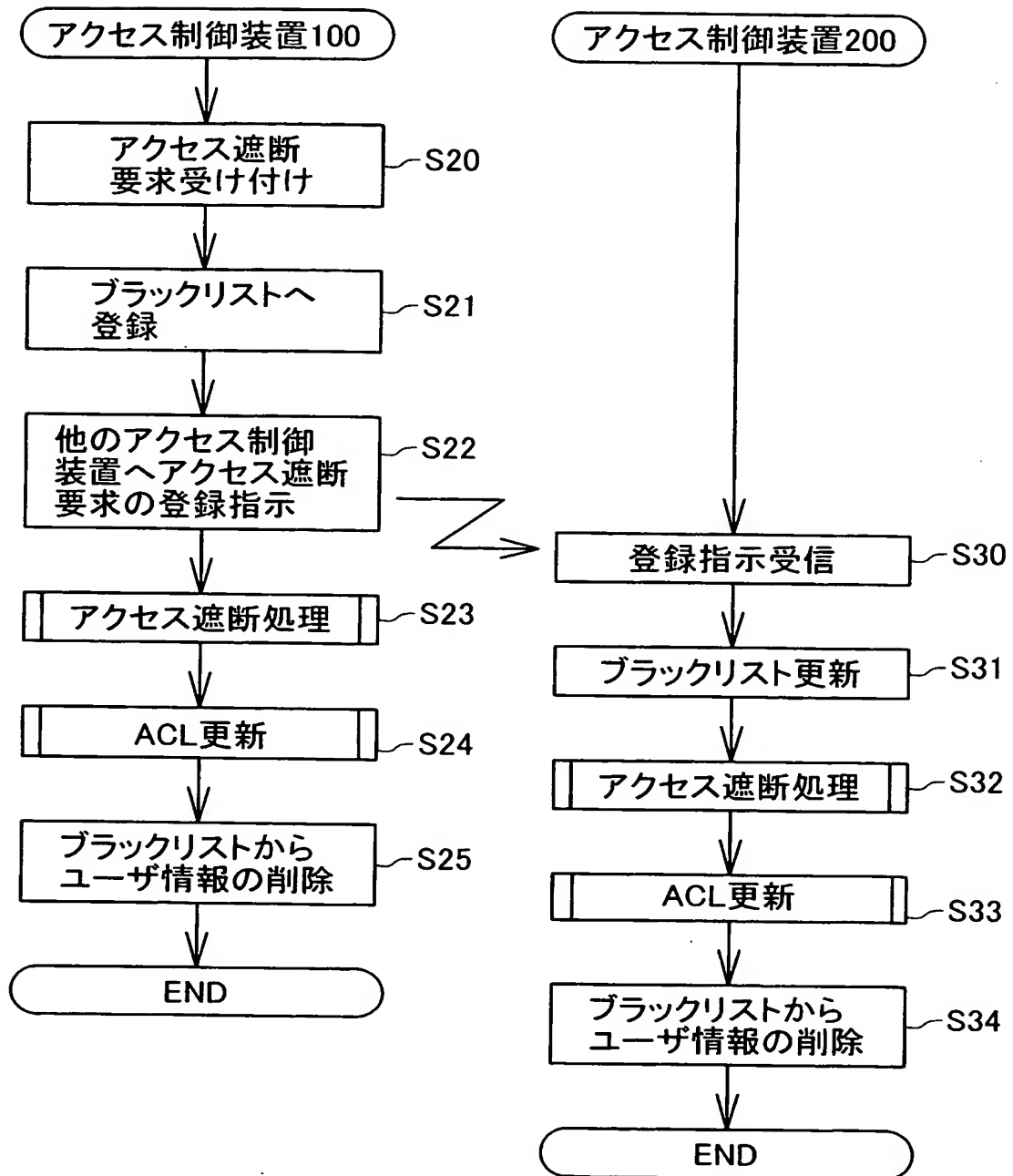
【図 5】



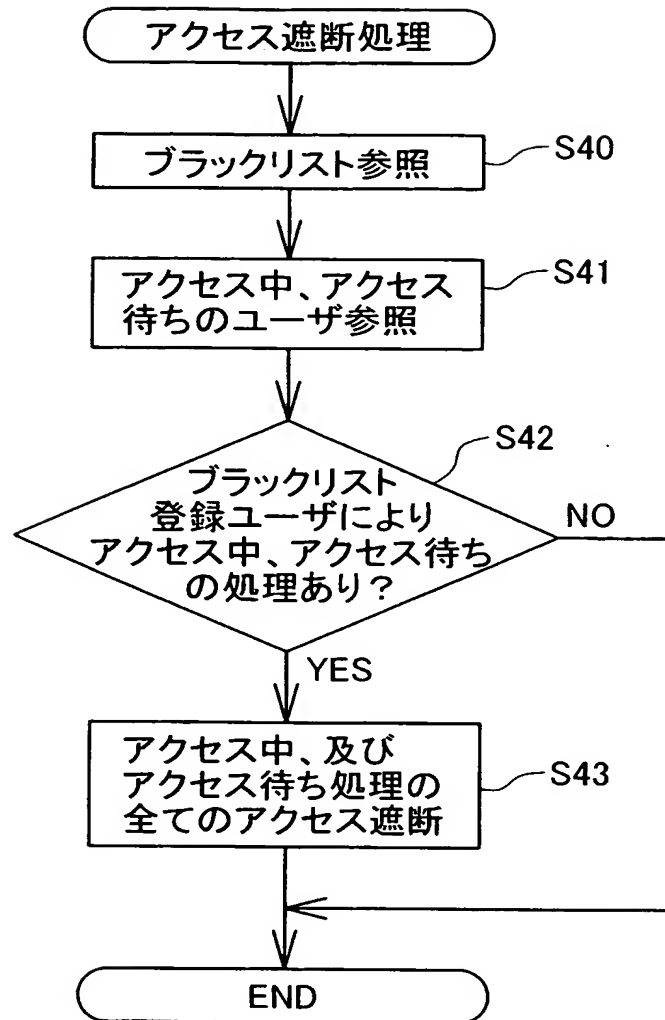
【図 6】



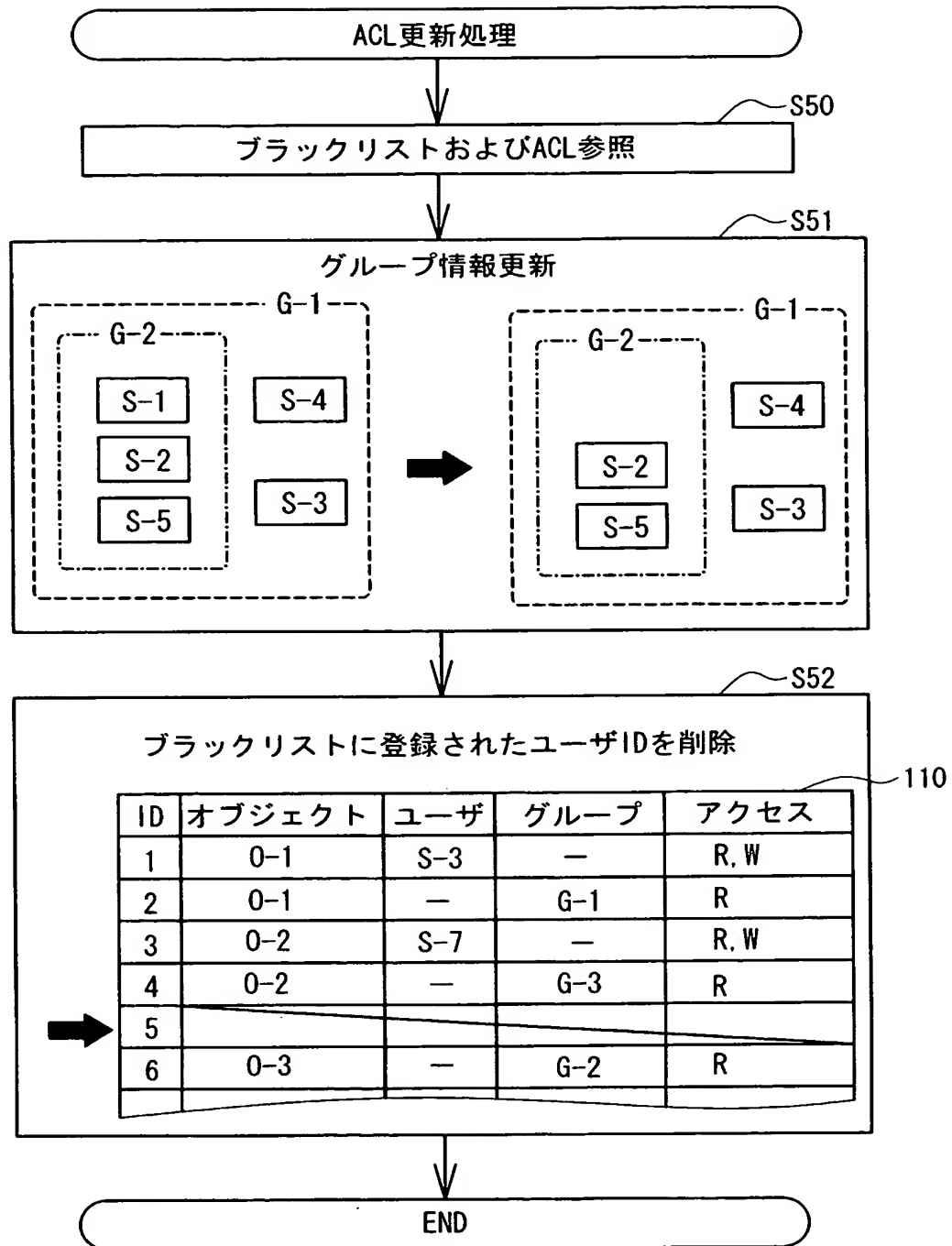
【図 7】



【図 8】

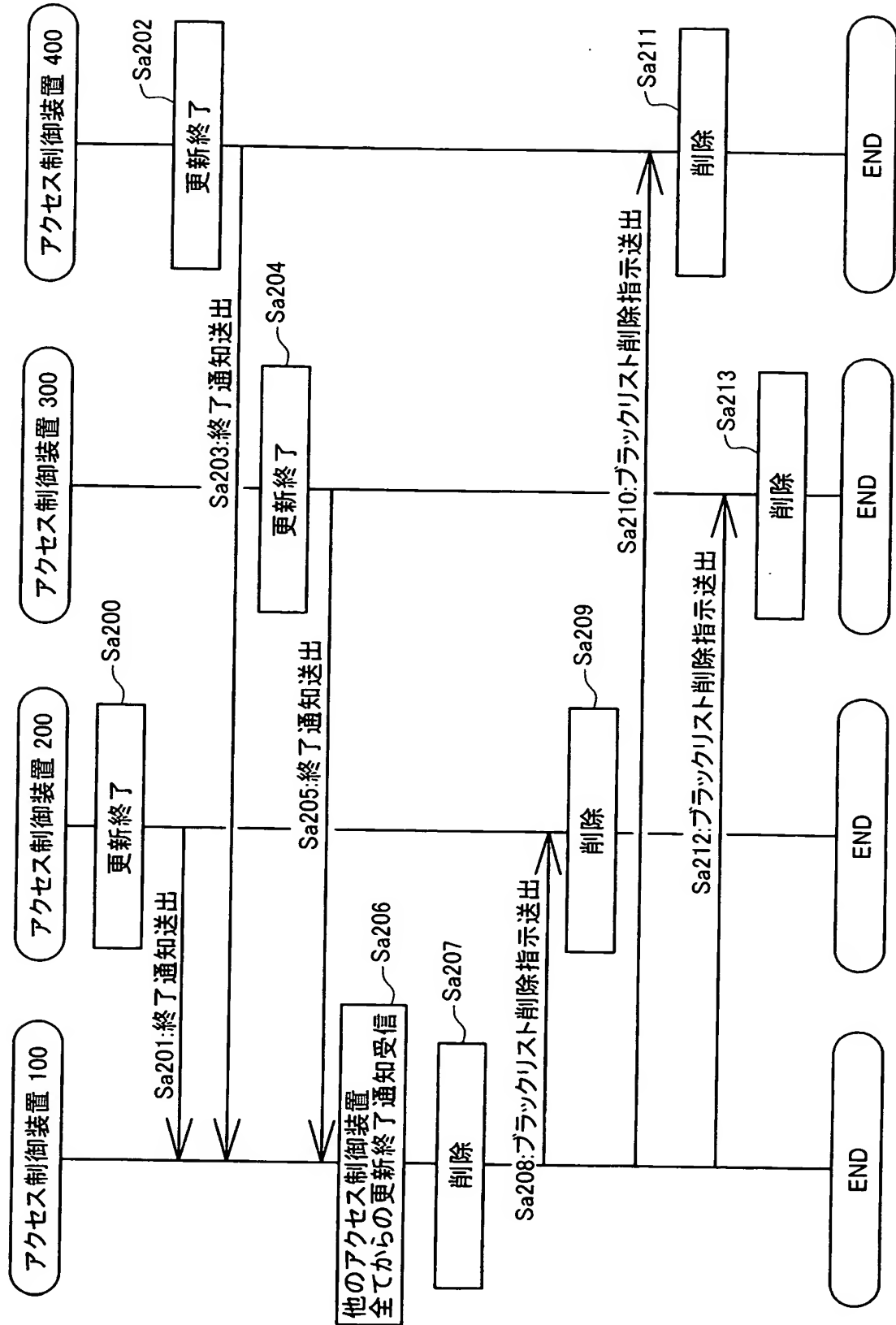


【図 9】

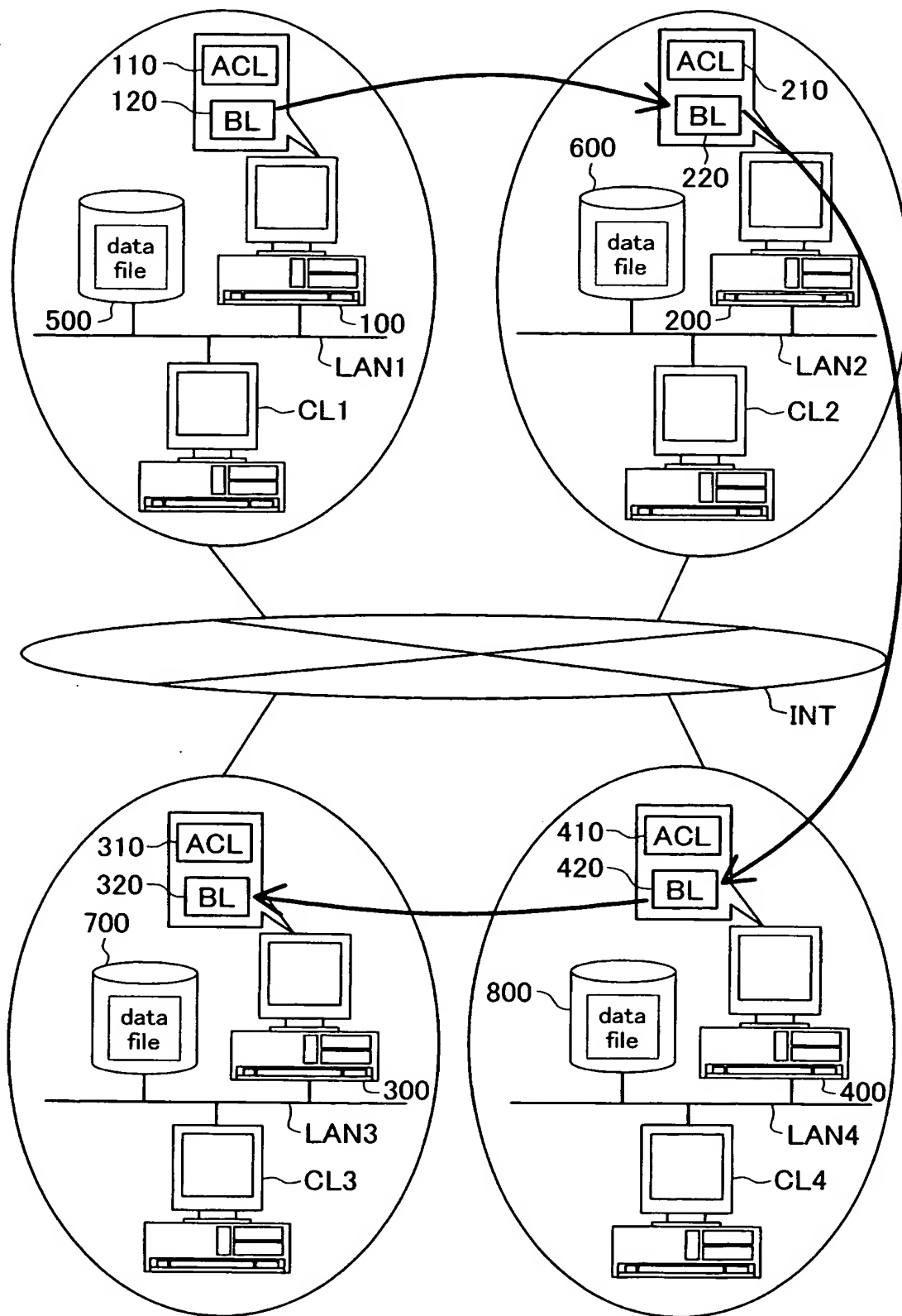




【図 10】



【図 11】



【書類名】 要約書

【要約】

【課題】 超分散環境において、緊急アクセス遮断を実現する。

【解決手段】 アクセス制御装置 100 は、オブジェクトのアクセス権限が設定されたアクセスコントロールリスト 110 (ACL 110) と、緊急アクセス遮断対象のユーザ情報が登録されたブラックリスト 120 (BL 120) とを管理している。アクセス制御装置 100 は、アクセス権限確認要求を受け、ACL 110 に先立ち BL 120 でアクセス可否を判断し、BL 120 でアクセス拒否されていない場合には ACL 110 でアクセス可否を判断する。アクセス制御装置 100 は、アクセス遮断対象のユーザ情報を他のアクセス制御装置に、各ブラックリストへの登録指示とともに配信する。本発明により、超分散環境において、緊急アクセス遮断を必要とするユーザが発生した場合にも、全てのネットワークで効率的に緊急アクセス遮断を行うことができる。

【選択図】 図 1

特願 2 0 0 3 - 3 8 9 2 3 0

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 1 0 8 ]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所